APPENDIX: AMENDED PORTIONS OF SPECIFICATION AND CLAIMS – MARKED TO SHOW CHANGES

SPECIFICATION:

First complete paragraph on page 2 of the Application:

Conventionally, the associated rules are executed manually. However, such manual execution has limitations related to timeliness and consistency. With regard to timeliness, it is often desired to selectively share information in contexts where timeliness of dissemination is critical. For example, the positions of friendly and potentially hostile military assets may need to be quickly distributed to decision-makers in the field. However, such decision-makers may have various clearances related to their service association, alliance affiliation or nationality and the like. In an era of active international police efforts, the need to simultaneously share information and protect national security interests is particularly challenging and important. Manually reviewing volumes of messages against a complicated array of ~~sanitation~~ sanitization rules is time consuming and impractical for certain applications. Moreover, manual administration of rules introduces an undesirable element of human subjectivity and inconsistency into an area where uniformity is of paramount importance.

First paragraph in the "Summary of the Invention":

The present invention is directed to a machine-based method and apparatus (collectively "utility"), for sanitizing messages based on stored ~~sanitation~~ sanitization rules. The utility can quickly and accurately apply the ~~sanitation~~ sanitization rules thereby accelerating the distribution of messages. In addition, the utility can apply a variety of rules depending on the context of a message, thus providing particular advantages in an MLS environment. The utility can also analyze messages with a high degree of resolution to maximize transmission of clean information while protecting sensitive subject matter. Moreover, the utility can flexibly handle a variety of source formats, including

imaging and text formats, as well as a variety of target formats without undue delays associated recompiling and the like.

IN THE CLAIMS:

1. (Amended) A method for use in a multi-level secure system for sanitizing a message, said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive, said method comprising the steps of:

establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules;

~~operating~~ using said computer-based sanitization tool to receive a first message from a first external system ~~associated with said first security level~~, said first message including said sensitive information and additional information;

first operating said computer-based sanitization tool to identify said sensitive information within said message and to sanitize said message relative to said sensitive information, thereby generating a first sanitized message different than said first message; and

second operating said computer-based sanitization tool for transmission of said first sanitized message to a second external system, said second external system being associated with said second security level.

2. (Added) A method as set forth in Claim 1, wherein said step of first operating comprises identifying said sensitive information based on said second security level and protecting said sensitive information such that said sensitive information is not useable by said second external system.

3. (Added) A method as set forth in Claim 1, wherein said step of first operating comprises accessing storage including multiple rule sets, using a parameter associated with said second security level to select a rule set, and

applying said selected rule set with respect to the first message to generate said first sanitized message.

4. (Added) A method as set forth in Claim 1, wherein said step of second operating comprises identifying a third external system associated with a third security level, operating said computer-based sanitization tool to generate a second sanitized message different than each of said first message and said first sanitized message, and operating said computer based sanitization tool for transmission of said second sanitized message to said third external system.

5. (Added) A method as set forth in Claim 1, wherein said step of using comprises receiving a text only message.

6. (Added) A method as set forth in Claim 1, wherein said first message includes a graphics portion and said step of first operating comprises protecting sensitive information within said graphics portion such that said sensitive information is not useable by said second external system.

7. (Added) A method as set forth in Claim 1, wherein said step of first operating comprises parsing said first message into a number of tokens and separately analyzing each token for said sensitive information.

8. (Added) A method as set forth in Claim 1, wherein said step of first operating comprises recursively parsing said first message to provide tokens of progressively smaller content until a desired parsing resolution is achieved and separately analyzing each token of said desired parsing resolution for said sensitive information.

9. (Added) A method as set forth in Claim 1, wherein said step of second operating comprises identifying a first format associated with said second external system and converting said first sanitized message into said first format.

10. (Added) A method as set forth in Claim 1, wherein said step of second operating comprises identifying a first format associated with said second external system, accessing storage including multiple specifications relating to multiple formats, retrieving from said storage first specification information for said first format and converting said first sanitized message into said first format using said first specification information.

11. (Added) A method as set forth in Claim 1, further comprising the steps of generating a second sanitized message, the same or different than the first sanitized message, for transmission to a third external system, where said second external system is associated with a first format and said third external system is associated with a second format, first converting said first sanitized message into said first format and second converting said second sanitized message into said second format.

12. (Added) A method as set forth in Claim 11, further comprising the step of providing storage including first specification information for said first format and second specification information for said second format, where said step of first converting comprises accessing said storage to obtain said first specification information and said step of second converting comprises accessing said storage to obtain said second specification information, wherein said storage can be used to reconfigure said sanitization tool for transmission in multiple formats without re-compiling.

13. (Added) A method for use in a multi-level secure system for sanitizing a message, said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive, said method comprising the steps of:

establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules;

first using said computer-based sanitization tool for receiving a message for potential distribution;

second operating said computer-based sanitization tool for identifying at least first and second potential recipients having first and second security clearances, respectively;

third operating said computer-based sanitization tool for sanitizing said received message to generate a first sanitized message for transmission to said first potential recipient; and

fourth operating said computer-based sanitization tool for sanitizing said received message to generate a second sanitized message, different than the first sanitized message, for transmission to said second potential recipient.

14. (Added) A method as set forth in Claim 13, wherein said step of third operating comprises identifying first sensitive information within said message based on said first security clearance of said first potential recipient and protecting said first sensitive information such that said first sensitive information is not useable by said first potential recipient, and said step of fourth operating comprises identifying second sensitive information based on said second security clearance of said second potential recipient and protecting said second sensitive information such that said second sensitive information is not useable by said second potential recipient.

15. (Added) A method as set forth in Claim 13, wherein said step of third operating comprises accessing storage including multiple rule sets, using a parameter associated with said first security clearance to select a first rule set, and applying said selected first rule set with respect to said message to generate said first sanitized message, and said step of fourth operating comprises accessing said storage including said multiple rule sets, using a second parameter associated with said second security clearance to select a second rule set, and applying said second rule set with respect to said message to generate said second sanitized message.

16. (Added) A method as set forth in Claim 13, wherein said step of first using comprises receiving a text only message.

17. (Added) A method as set forth in Claim 13, wherein said message includes a graphics portion and said step of third operating comprises protecting sensitive information within said graphics portion such that said sensitive information is not useable by said first recipient.

18. (Added) A method as set forth in Claim 13, wherein said step of third operating comprises parsing said message into a number of tokens and separately analyzing each token for sensitive information.

19. (Added) A method as set forth in Claim 13, wherein said step of third operating comprises identifying a first format associated with said first potential recipient and converting said first sanitized message into said first format, and said step of fourth operating comprises identifying a second format associated with said second potential recipient and converting said second sanitized message into said second format.

20. (Added) A method as set forth in Claim 19, further comprising the step of providing storage including first specification information for said first format and second specification information for said second format, where said step of third operating comprises accessing said storage to obtain said first specification information and said step of fourth operating comprises accessing said storage to obtain said second specification information, wherein said storage can be used to reconfigure said sanitization tool for transmission in multiple formats without re-compiling.

21. (Added) A method for use in a multi-level secure system for sanitizing a message, said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive

sensitive information that second security level users are not authorized to receive, said method comprising the steps of:

establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules;

first operating said computer-based sanitization tool for receiving a message and recursively parsing the message such that the message is parsed into tokens of a desired size;

second operating said computer-based sanitization tool for applying sanitization rules with respect to the parsed tokens to identify at least one dirty token relative to an identified recipient; and

third operating said computer-based sanitization tool for sanitizing said message relative to said dirty token to generate a sanitized message for transmission to said identified recipient.

22. (Added) A method as set forth in Claim 21, wherein said step of second operating comprises identifying said at least one dirty token based on a security level associated with said identified recipient and protecting said dirty token such that said dirty token is not useable by said identified recipient.

23. (Added) A method as set forth in Claim 21, wherein said step of second operating comprises accessing storage including multiple rule sets and using a parameter associated with said identified recipient to select said sanitization rules.

24. (Added) A method as set forth in Claim 21, wherein said step of first operating comprises receiving a text only message.

25. (Added) A method as set forth in Claim 21, wherein said message includes a graphics portion and said step of second operating comprises identifying said at least one dirty token within said graphics portion.

26. (Added) A method as set forth in Claim 21, wherein said step of third operating comprises identifying a format associated with said identified recipient and converting said sanitized message into said format.

27. (Added) An apparatus for use in a multi-level secure system for sanitizing a message, said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive, said apparatus comprising:

an interface engine including a generic processing module for performing a transformation process relative to an information stream associated with an external system, said generic processing module being adaptable to handle messages in multiple forms associated with multiple external systems;

a storage structure for storing at least first external specification information relating to a first external form of a first external system and second external specification information relating to a second external form of a second external system;

said interface engine being operative to identify an external form associated with a message and accessing said storage to obtain a corresponding specification;

second storage structure for storing sanitization rules; and

a sanitization engine operative for accessing said second storage structure to obtain at least one sanitization rule and for sanitizing said message based on said at least one sanitization rule.

28. (Added) An apparatus as set forth in Claim 27, wherein said interface engine is operative to identify said external form based on an intended recipient of said message, to access said storage structure to obtain external specification information associated with said recipient and to convert said sanitized message into said external form.

29. (Added) An apparatus as set forth in Claim 27, wherein said sanitization engine is operative for identifying a potential recipient of said message and obtaining said at least one sanitization rule based on said intended recipient.